Workshop:

Advanced Active Directory Attacks

CQURE

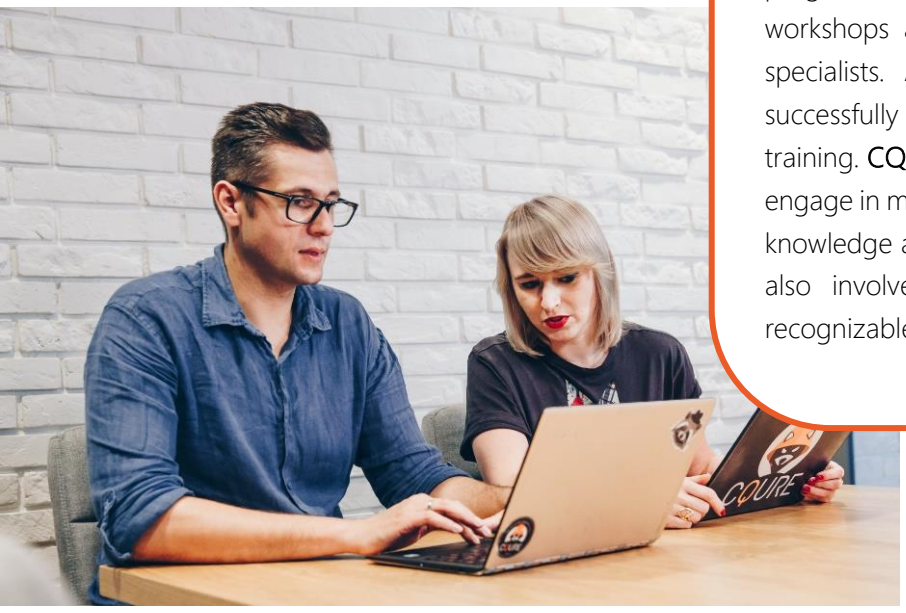
Warsaw New York Dubai Zug

info@cqure.pl

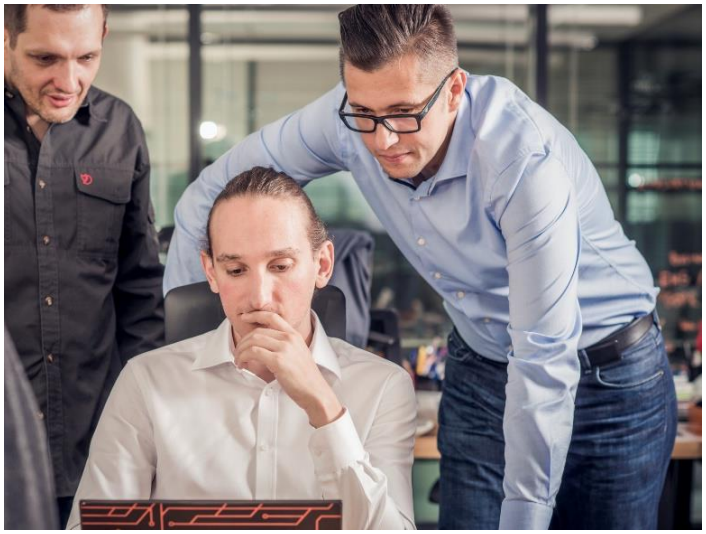
www.cqure.pl
www.cqureacademy.com

Paula Januszkiewicz is a world-renowned cybersecurity Expert, a founder of CQURE and CQURE Academy, and Microsoft Regional Director and MVP.

CQURE Academy focuses on cybersecurity training program consisting of over 20 high-quality technical workshops and seminars and providing certification to specialists. Additionally, in October 2016 CQURE has successfully launched online and subscription-based training. **CQURE Experts** speak at international events and engage in multiple cybersecurity projects – they bring their knowledge and experience to trainings. CQURE Academy also involves R&D – that is why CQURE Team is recognizable in the cybersecurity field.



This is just a great workshop that teaches how to implement secure Microsoft Active Directory infrastructure. The course covers all modern attacks against core Windows identity solutions that everybody talks about and during the session you will learn how to prevent them! Our goal is to show you how to make your AD infrastructures secure based attacker's possibilities.



About the course

This is a deep dive workshop on Active Directory services security, a must-go for administrators, security officers and architects. It is delivered by one of the best people in the market in the security field – with practical knowledge from tons of successful projects, many years of real-world experience, great teaching skills and no mercy for misconfigurations or insecure solutions. This workshop will present you the critical tasks performed by skilled attacker or pentester against Active Directory and its key components. Course focus on attacks and security of Windows identity solutions.

We really want you to leave the workshop with practical, ready-to-use knowledge of how to get into the infrastructure!

Exploits are not the only way to get to the systems! We will go through the operating systems' built-in problems and explore how they can be beneficial for hackers! One of the most important things to conduct a successful attack is to understand how the targets work. *To the bones*! Afterwards everything is clear and the tool is just a matter of our need.

The workshop covers all aspects of Active Directory identity security from the hacker's mind perspective! Our goal is to show and teach you what kind of mechanisms are allowing to get inside the infrastructure and how to get into organization. **You will gain penetration tester's knowledge and tools.**

The course is an intense workshop! During these 3 days you will not need your caffeine candies – this workshop is really intense and it will keep you awake all the time!

All exercises are based on **Windows Server 2016 and 2019, Windows 10**, Kali Linux and **Azure Cloud**. This workshop is based on practical knowledge from tons of successful projects, many years of real-world experience and no mercy for misconfigurations or insecure solutions!

Prerequisites:

To attend this training, you should have a good hands-on experience in administering Windows infrastructure. At least 5 years in the field is recommended.

Target audience

Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.

Materials

Author's unique tools, presentations slides.

Agenda

Module 1: Authentication protocols

a) NTLM

b) Kerberos

c) Claim based authentication

Module 2: Identity attacks

a) Pass-the-Hash attacks

b) Stealing the LSA Secrets

c) Modern identity attacks techniques

d) Password guessing, spraying a brute-forcing

e) MITM attacks, NBNS/LLMNR spoofing, NTLM Relay, Kerberoasting

f) Offline attacks, decrypting DPAPI a DPAPI-NG

g) Attacks against smart card authentication

Module 3: Active Directory attacker persistency

a) Achieving persistence, Skeleton Key, Golden Ticket attack

b) Windows Hello for Business Security, NGC keys

c) DCSync and DCShadow

d) AdminSDholder

Module 4: Mitigating the identity attacks

a) Pass-the-Hash attack prevention

b) LSA protection

c) Credential Guard

Module 5: Azure AD security

a) Stealing Azure AD tokens

b) Azure MFA and FIDO2 auditing

c) Azure AD application security